

REMARKS

In response to the final Office Action dated October 27, 2008, reconsideration and allowance of the above-identified application are respectfully requested. Claims 1 and 3-20 remain pending.

Claims 1 and 3-20 are rejected under 35 U.S.C. § 103(a) as being obvious in view of the combination of U.S. Patent No. 5,957,985 to Wong et al. ("Wong") and U.S. Patent No. 6,330,670 to England et al. ("England"). This ground of rejection is respectfully traversed.

Applicant's claim 1 recites a method that involves signing software against falsification using a secret key according to a public-key method, checking the signed software for integrity using the public key complimentary to the secret key, and generating a software signature certificate using the public key of a software signature site and a secret key of a control entity of a trust center, according to the public-key method. The combination of Wong and England does not disclose or suggest the claimed method.

The Office Action recognizes that Wong does not even mention signing software or checking the integrity of signed software, and instead relies upon England for such a disclosure. For at least the reasons set forth below, it is respectfully submitted that England does not remedy the deficiencies of Wong with respect to Applicant's claim 1.

THE DISCLOSURE OF ENGLAND

England discloses a digital rights management operating system for protecting rights-managed data from access by untrusted programs.¹ A central processing unit (CPU) executes a stored operating system.² The operating system includes a boot block which is used to authenticate the operating system during boot operation.³ The boot block loads drivers and software components necessary for an operating system to function and forms an identity of the operating system.⁴

England discloses a number of different certificates, including a manufacturer certificate 166, CPU certificate 202, and rights manager certificate 210. Using such certificates a content provider can determine whether a trust relationship can be established with the CPU and a digital rights management operating system (DRMOS). England however does not disclose **generating a software signature certificate** using:

- the public key of the software signature site; and
- a secret key of a control entity of a trust center, according to a public-key method.

¹ Abstract.

² Column 8, lines 30-37.

³ Id.

⁴ Column 11, lines 43-47.

THE OFFICE ACTION'S CITATIONS TO ENGLAND

The final Office Action cites column 7, line 63 – column 8, line 4 of England for the disclosure of the aforementioned elements of Applicant's claim 1. As will be described below in detail, however, there is nothing in these sections disclosing the aforementioned claim elements.

The first paragraph of this citation discloses that manufacturer certificate 166 testifies that the CPU was produced according to a known specification and, "that the manufacturer created the key pair 164, placed the key pair onto the CPU 140, and then destroyed its own knowledge of the private key K_{CPU}^{-1} ."

As can be seen from reviewing the cited portion of England, this portion discusses a CPU signature using public and private keys of the CPU. Accordingly, there is nothing in this section disclosing or suggesting *generating a software signature certificate using the public key of the software signature site or the secret key of the control entity* of the trust center.

The second paragraph of the citation in the Office Action discloses that, "manufacturer certificate 166 contains the manufacturer's public key K_{MFR} , the CPU's public key K_{CPU} , and the above testimony. The manufacture signs the certificate using its private signing key, K_{MFR}^{-1} ."

The Response to Arguments section of the Office Action states that, in England, the manufacturer is a software developer and that the CPU is a control entity. Even if it were assumed that this is an accurate characterization of

England, which it is not, England does not disclose or suggest that the manufacturer is, "a software signature site" or that the CPU is, "a control entity of a trust center."

Furthermore, Applicant's claim 1 recites that the certificate is generated using, "a secret key of a trust center."⁵ Again, even if it were assumed that CPU is, "a control entity of a trust center," England discloses that certificate 166 includes the public key of the CPU, K_{CPU}, and not the private key K_{CPU}¹.

Accordingly, England does not disclose or suggest generating a software signature certificate using the *public key of the software signature site* or the *secret key of the control entity of the trust center*, nor generating of a software signature certificate using the keys.

Because the rejection of Applicant's claim 1 relies upon England for the disclosure of generating the software signature certificate, it is respectfully submitted that the combination of Wong and England does not render Applicant's claim 1 obvious.

Applicant notes that the Response to Arguments section inaccurately characterizes England. Specifically, this section of the Office Action states that:

The England prior art discloses a mechanism to protect content such as software. The software includes software developed for the operation of a control unit used in a vehicle.

⁵ Emphasis added.

England, however, makes no mention that the operating system or the CPU is used in a vehicle. Accordingly, this alleged disclosure by England should not be considered in determining whether Applicant's claims are obvious.

Dependent claims 3-6 and 8-18 are patentably distinguishable over the combination of Wong and England at least by virtue of their dependency from claim 1.

Independent claim 7 recites a method involving software signature certificate, and is patentably distinguishable over the combination of Wong and England for similar reasons to those discussed above with regard to claim 1.

Regarding Applicant's independent claim 19, the Office Action cites disclosure in column 12, lines 27-30 of England for checking if the software signature certificate has been changed or manipulated. A disclosure of revocation of a particular version of a plug and play component, based solely on the version, does not, however, disclose or suggest checking a software signature certificate as recited in claim 19. Claim 20 is patentably distinguishable over the combination of Wong and England at least by virtue of its dependency from claim 19.

Claim 20 is rejected under 35 U.S.C. § 112, second paragraph for indefiniteness. The Office Action alleges that there is no disclosure of a third public key and a third signature. Applicant's respectfully submit that this is not

a proper rejection under U.S.C. § 112, second paragraph. If a description or the enabling disclosure of a specification is not commensurate in scope with the subject matter encompassed by a claim, that fact alone does not render the claim imprecise or indefinite or otherwise not in compliance with 35 U.S.C. § 112, second paragraph.⁶ Applicant respectfully submit that Fig. 1 of Applicant's disclosure discloses a trust center signature certificate 116 comprising a key 101 and signature 117 (e.g., first key and first signature), clearing code site software signature certificate 118 comprising a key 106 and signature 119 (e.g., second key and second signature), and software signature certificate 120 comprising a key 108 and signature 121 (e.g., third key and third signature). Accordingly, withdrawal of this rejection is respectfully requested.

Finally, Applicant notes that the Response to Arguments section inaccurately characterizes Applicant's previous arguments and Applicant's claims. For example, this section states, "Applicant argues that the referenced prior art does not disclose, specification objection." Applicant's Reply contained no references to the prior art with respect to this rejection and objection. Similarly, this section quotes Applicant's previous Reply as stating, "England is not an analogous reference." This exact language does not appear in Applicant's previous Reply, and therefore should not be enclosed in quotes.

Regarding Applicant's claims, this section discusses what the "claimed invention appears to be." Applicant's claimed invention is defined by the actual

⁶ MPEP 2174.

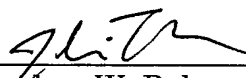
language of the claim and not this inaccurate characterization that attempts to improperly distill the claims into what the Examiner considers as the "gist" of the invention.

If there are any questions regarding this response or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and please charge any deficiency in fees or credit any overpayments to Deposit Account No. 05-1323 (Docket # 080437.53236US).

Respectfully submitted,

January 23, 2009



Stephen W. Palan
Registration No. 43,420
John P. Teresinski
Registration No. 56,621

CROWELL & MORING, LLP
Intellectual Property Group
P.O. Box 14300
Washington, DC 20044-4300
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
SWP:JPT/cee
6694997